(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－20956

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｆ	
	9/06	５５０			9/06	５５０Ａ	
						５５０Ｚ	
	13/00	３５１			13/00	３５１Ｅ	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ	

審査請求　未請求　請求項の数23　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願平8－170106

(22)出願日　平成８年(1996)６月28日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　田中　利治
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

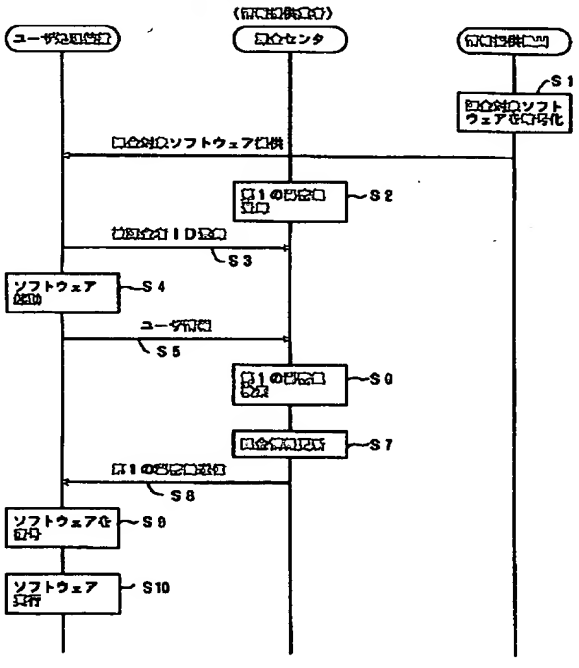
(54)【発明の名称】　ソフトウェア課金方法及びシステム

(57)【要約】

【課題】　ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。

【解決手段】　被課金者がソフトウェアを起動し、ユーザ情報を課金センタに送信すると、課金センタはソフトウェアの使用料及び第１の復号・秘密鍵を検索することにより取得し、被課金者ＩＤに対応する課金情報を更新し、取得した第１の復号・秘密鍵をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから受信した第１の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し、実行する。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】　ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、

情報提供機関は、

被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し、

課金センタは、

課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を登録しておき、

前記被課金者は、前記課金センタに被課金者ＩＤを登録しておき、

前記被課金者がソフトウェアを起動して、該ソフトウェアＩＤを含む該ソフトウェア使用通知を前記課金センタに送信すると、

前記課金センタは、前記ソフトウェア使用通知に基づいて前記ソフトウェアの使用料及び前記第１の復号・秘密鍵を検索し、

前記ソフトウェア使用料で前記被課金者ＩＤに対応する課金情報を更新し、

取得した前記第１の復号・秘密鍵をユーザ処理装置に送信し、

前記ユーザ処理装置は、前記課金センタから受信した前記第１の復号・秘密鍵を用いて前記ソフトウェアの全部または、一部の暗号化されている領域を復号し、実行することを特徴とするソフトウェア課金方法。

【請求項２】　前記ユーザ処理装置は、

乱数を生成し、前記課金センタに、前記ソフトウェア使用通知と共に送信し、

前記課金センタは、

前記ユーザ処理装置から乱数を受信し、前記第１の復号・秘密鍵と共に受信した乱数を前記ユーザ処理装置に送信し、

前記ユーザ処理装置は、

前記課金センタから前記第１の復号・秘密鍵と前記乱数を受信し、

生成した前記乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみ前記ソフトウェアの復号を行う請求項１記載のソフトウェア課金方法。

【請求項３】　前記課金センタにおいて、

前記登録情報として、前記ソフトウェアに対応する前記第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、前記第２の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第１の復号・秘密鍵を暗号化した暗号化情報を前記ユーザ処理装置に送信し、

前記ユーザ処理装置では、

前記ソフトウェアに埋め込んである第２の秘密鍵を抽出し、

2

前記第２の秘密鍵を用いて、前記暗号化情報を復号して前記第１の復号・秘密鍵を取得し、

取得した前記第１の復号・秘密鍵を用いて前記ソフトウェアを復号する請求項１又は、２記載のソフトウェア課金方法。

【請求項４】　前記ユーザ処理装置は、

被課金者の第３の私的秘密鍵を用いて、前記課金センタに送信する情報の一部を暗号化することにより署名を生成して、前記課金センタに送信し、

前記課金センタは、

前記登録情報として、更に被課金者の第３の私的秘密鍵に対応した公開鍵を含み、前記署名を該公開鍵で復号した情報と、前記ユーザ処理装置から受信した他の情報と一致しているかを判定し、

一致する場合のみ前記第１の復号・秘密鍵を前記ユーザ処理処理装置に送信する請求項１、２、又は、３記載のソフトウェア課金方法。

【請求項５】　前記ユーザ処理装置では、

暗号化された前記ソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する請求項１、２、３、又は４記載のソフトウェア課金方法。

【請求項６】　前記ユーザ処理装置では、

前記暗号化されたソフトウェアを復号して実行する際に、

予め、復号したデータを格納するための領域を確保し、

前記ソフトウェアの実行開始時または、実行中に、前記暗号化されたソフトウェアの全部または、一部を復号して、前記復号したデータを格納する領域に格納し、

前記ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号したデータを格納する領域へのアクセスで代替する請求項１、２、３又は４記載のソフトウェア課金方法。

【請求項７】　前記ユーザ処理装置は、

前記課金センタに、前記ソフトウェアの機能ＩＤを前記ソフトウェア使用通知に付加して送信し、

前記課金センタは、

課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応した前記ソフトウェアを復号するための第４の復号・秘密鍵を登録情報として登録しておき、

前記ユーザ処理装置から送信された前記ソフトウェアＩＤ、及び前記機能ＩＤを用いて、前記登録情報を検索し、機能使用料及び、前記第４の復号・秘密鍵を取得し、

前記被課金者ＩＤ、及び前記機能使用料を用いて、前記ユーザ情報を検索して、該被課金者ＩＤに対応した課金情報を更新する請求項１、２、３、４、５又は、６記載のソフトウェア課金方法。

【請求項８】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアのアドレス範囲内のデータを暗号化する請求項１記載のソフトウェア課金方法。
【請求項９】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの機能単位で暗号化する請求項１記載のソフトウェア課金方法。
【請求項１０】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する請求項１記載のソフトウェア課金方法。
【請求項１１】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、
分割された各々の副領域を異なる秘密鍵で暗号化する請求項１０記載のソフトウェア課金方法。
【請求項１２】　提供されたソフトウェアを使用するユーザ処理装置と、該ユーザ処理装置が使用するソフトウェアについて課金処理を行う課金センタと、該ユーザ処理装置及び該課金センタを接続するネットワークからなるソフトウェア課金システムであって、
前記ユーザ処理装置に対して提供するソフトウェアを第１の復号・秘密鍵を用いて暗号化する第１の暗号化手段と、
暗号化されたソフトウェアを前記ユーザ処理装置に提供するソフトウェア提供手段とを有する情報提供機関を含み、
前記課金センタは、
前記ユーザ処理装置から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置が使用するソフトウェアに対する課金を行う課金手段と、
前記課金処理が終了した時点で、前記第１の暗号化手段で用いられた前記第１の復号・秘密鍵を前記ユーザ処理装置に送信する復号鍵送信手段とを有し、
前記ユーザ処理装置は、
予め、前記課金センタに対して自装置ＩＤを登録するＩＤ登録手段と、
配付されたソフトウェアを使用するソフトウェア使用通知を前記課金センタに通知する使用通知手段と、
前記課金センタから受信した前記第１の復号秘密鍵を用いて、前記ソフトウェア全部、または、一部の暗号化されている領域を復号し、実行する第１の復号手段とを有することを特徴とするソフトウェア課金システム。
【請求項１３】　前記課金センタの前記課金手段は、
課金対象となるソフトウェア毎に、ソフトウェアＩＤ、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を格納するための課金情報記憶手段と、
前記ユーザ毎に、被課金者ＩＤ及び、ユーザ課金情報を保持するユーザ情報記憶手段と、
前記ソフトウェアＩＤを用いて、前記課金情報記憶手段を検索して、ソフトウェア使用料、及び第１の復号・秘密鍵を取得する第１の検索手段と、
前記ユーザ処理装置から前記使用通知手段により送信された被課金者ＩＤに基づいて前記ユーザ情報記憶手段を検索し、該被課金者ＩＤに対応するユーザ課金情報を取得して、前記ソフトウェア使用料で更新する第１の課金情報更新手段とを含む請求項１２記載のソフトウェア課金システム。
【請求項１４】　前記ユーザ処理装置の前記通知手段は、
乱数を生成する乱数生成手段と、
前記課金センタに、前記ソフトウェア使用通知と共に、前記乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、
前記第１の復号手段は、
前記課金センタから受信する乱数と前記乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、
前記課金センタの前記復号鍵送信手段は、
前記乱数送信手段により前記ユーザ処理装置から受信した前記乱数を前記第１の復号・秘密鍵と共に送信する乱数送信手段を含む請求項１２又は１３記載のソフトウェア課金システム。
【請求項１５】　前記課金センタの前記課金情報記憶手段は、
前記ソフトウェアに対応する前記第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、
前記復号鍵送信手段は、
前記第２の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第１の復号・秘密鍵を暗号化した暗号化情報を生成する第２の暗号化手段を含み、
前記ユーザ処理装置の第１の復号手段は、
前記課金センタから受信した前記暗号化情報を、前記ソフトウェアに埋め込んである第２の秘密鍵を抽出し、前記暗号化情報を該第２の秘密鍵で復号して、該第１の復号・秘密鍵を取得し、該第１の復号・秘密鍵で前記ソフトウェアを復号する第２の復号化手段を含む請求項１２、１３又は、１４記載のソフトウェア課金システム。
【請求項１６】　前記ユーザ処理装置の使用通知手段は、
被課金者の第３の私的秘密鍵を用いて、前記課金センタに送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、
前記課金センタに送信する前記ソフトウェア使用通知と共に署名を前記課金センタに送信する署名送信手段を更に有し、
前記課金センタは、

5

前記ユーザ情報記憶手段に、被課金者の第３の私的秘密鍵に対応した公開鍵を含み、
前記ユーザ情報記憶手段上の前記被課金者の第３の私的秘密鍵に対応し、署名を復号するための公開鍵を用いて、前記ユーザ処理装置から受信した前記署名を復号し、該ユーザ処理装置から受信した前記ソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する請求項１２、１３、１４又は１５記載のソフトウェア課金システム。

【請求項１７】　前記第１の復号化手段は、
命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む請求項１２、１３、１４、１５又は１６記載のソフトウェア課金システム。

【請求項１８】　前記第１の復号化手段は、
予め復号したデータを格納する復号データ格納手段と、前記ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して前記復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号データ格納手段へのアクセスで代替する代替アクセス手段を含む請求項１２、１３、１４、１５又は１６記載のソフトウェア課金システム。

【請求項１９】　前記課金センタは、
課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応し、前記ユーザ処理装置に送信され、該課金対象ソフトウェアを復号するための第４の復号・秘密鍵を格納する第２の課金情報記憶手段と、
前記ソフトウェアＩＤ及び前記機能ＩＤを用いて、前記第２の課金情報記憶手段を検索して、機能使用料及び第４の復号・秘密鍵を取得する第２の検索手段と、
前記被課金者ＩＤ及び前記機能使用料を用いて、前記ユーザ情報記憶手段を検索して、前記被課金者ＩＤに対応したユーザ課金情報を更新する第２の課金情報更新手段を更に有し、
前記ユーザ処理装置は、
被課金者ＩＤ及びソフトウェアＩＤと共に、機能ＩＤを前記課金センタに送信するＩＤ通知手段を更に有する請求項１２、１３、１４、１５、１６、１７または、１８記載のソフトウェア課金システム。

【請求項２０】　前記情報提供機関の前記第１の暗号化手段は、
前記ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

【請求項２１】　前記情報提供機関の前記第１の暗号化手段は、
前記ソフトウェアの機能単位で暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

6

【請求項２２】　前記情報提供機関の前記第１の暗号化手段は、
前記ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

【請求項２３】　前記情報提供機関の前記第１の暗号化手段は、
前記ユーザ処理装置に提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する手段を含む請求項２２記載のソフトウェア課金システム。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、ソフトウェア課金方法及びシステムに係り、特に、ＣＤ－ＲＯＭやフロッピーディスク等の媒体に格納されて配付されるソフトウェアや、ネットワークを介して配付されるソフトウェアに対して課金を行うソフトウェア課金方法及びシステムに関する。

【０００２】
【従来の技術】従来のソフトウェア課金システムには、ソフトウェアを販売し、ユーザが当該ソフトウェアを買い取られた時点で課金が終了する方法がある。また、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知し、これにより、課金センタでは、ソフトウェアの使用に対する課金を行うシステムがある。

【０００３】また、最近では、買い取り形式の変形として暗号化されたソフトウェアをＣＤ－ＲＯＭ等の媒体または、ネットワーク経由で配付し、電話、ファクシミリ、手紙または、電子メールによる購入手続き後、復号鍵を通知する方式も採用されている。さらに、予め利用可能日が設定され、かつ、暗号化されたソフトウェアを配付して、ユーザが使用した日を日数で管理し、当該日数に基づいて課金を行う方法等がある。

【０００４】
【発明が解決しようとする課題】しかしながら、上記の買い取り方式では、流通経費を相対的に低減するためにソフトウェアの機能は肥大化し、ユーザは、殆ど使用しない機能を含め、高額の費用を負担しなければならない。また、ソフトウェアを購入して実行してみなければユーザが必要とする機能が満足されているか否かを判断できない。

【０００５】また、単に、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知する方法では、課金は可能であってもソフトウェアの使用を制限することができないため、使用料金の未払いがあっても対処することができないという問題がある。

【０００６】暗号化されたソフトウェアを予め提供し、

使用時に復号鍵を提供するシステムであっても、使用回数に関わらず、ユーザは、同一の金額を支払う必要があり、使用回数または、使用時間当たりの価格には大きな幅がある。本発明は、上記の点に鑑みなされたもので、ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。

【０００７】詳しくは、ソフトウェアの使用要求に対して、ユーザ課金情報を更新した後、使用許可を与え、使用許可されたソフトウェアがただ１回だけ使用可能であることを保障し、１回当たりの使用料を安価にすることが可能なソフトウェア課金方法及びシステムを提供することである。

【０００８】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。本発明は、ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、情報提供機関は、被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し（ステップ１）、課金センタは、課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を登録しておき（ステップ２）、被課金者は、課金センタに被課金者ＩＤを登録しておき（ステップ３）、被課金者がソフトウェアを起動して（ステップ４）、該ソフトウェアＩＤを含む該ソフトウェア使用通知を課金センタに送信すると（ステップ５）、課金センタは、ソフトウェア使用通知に基づいてソフトウェアの使用料及び第１の復号・秘密鍵を検索し（ステップ６）、ソフトウェア使用料で被課金者ＩＤに対応する課金情報を更新し（ステップ７）、取得した第１の復号・秘密鍵をユーザ処理装置に送信し（ステップ８）、ユーザ処理装置は、課金センタから受信した第１の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し（ステップ９）、実行する（ステップ１０）。

【０００９】また、本発明において、ユーザ処理装置は、乱数を生成し、課金センタに、ソフトウェア使用通知と共に送信し、課金センタは、ユーザ処理装置から乱数を受信し、第１の復号・秘密鍵と共に受信した乱数をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから第１の復号・秘密鍵と乱数を受信し、生成した乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみソフトウェアの復号を行う。

【００１０】また、本発明は、課金センタにおいて、登録情報として、ソフトウェアに対応する第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、第２の秘密鍵を用いて、ユーザ処理装置に送信する第１の復号・秘密鍵を暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、ソフトウェアに埋め込んである第２の秘密鍵を抽出し、第２の秘密鍵を用いて、暗号化情報を復号して第１の復号・秘密鍵を取得し、取得した第１の復号・秘密鍵を用いてソフトウェアを復号する。

【００１１】また、本発明において、ユーザ処理装置は、被課金者の第３の私的秘密鍵を用いて、課金センタに送信する情報の一部を暗号化することにより署名を生成して、課金センタに送信し、課金センタは、登録情報として、更に被課金者の第３の私的秘密鍵に対応した公開鍵を含み、署名を該公開鍵で復号した情報と、ユーザ処理装置から受信した他の情報と一致しているかを判定し、一致する場合のみ第１の復号・秘密鍵をユーザ処理処理装置に送信する。

【００１２】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する。

【００１３】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して実行する際に、予め、復号したデータを格納するための領域を確保し、ソフトウェアの実行開始時または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して、復号したデータを格納する領域に格納し、ソフトウェアの実行中の復号対象領域へのアクセスは、復号したデータを格納する領域へのアクセスで代替する。

【００１４】また、本発明において、ユーザ処理装置は、課金センタに、ソフトウェアの機能ＩＤをソフトウェア使用通知に付加して送信し、課金センタは、課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応したソフトウェアを復号するための第４の復号・秘密鍵を登録情報として登録しておき、ユーザ処理装置から送信されたソフトウェアＩＤ、及び機能ＩＤを用いて、登録情報を検索し、機能使用料及び、第４の復号・秘密鍵を取得し、被課金者ＩＤ、及び機能使用料を用いて、ユーザ情報を検索して、該被課金者ＩＤに対応した課金情報を更新する。

【００１５】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアのアドレス範囲内のデータを暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの機能単位で暗号化する。

【００１６】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割さ

れた各々の副領域を異なる秘密鍵で暗号化する。

【００１７】図２は、本発明の原理構成図である。本発明は、提供されたソフトウェアを使用するユーザ処理装置１００と、該ユーザ処理装置１００が使用するソフトウェアについて課金処理を行う課金センタ２００と、該ユーザ処理装置１００及び該課金センタ２００を接続するネットワークからなるソフトウェア課金システムであって、ユーザ処理装置１００に対して提供するソフトウェアを第１の復号・秘密鍵を用いて暗号化する第１の暗号化手段と、暗号化されたソフトウェアをユーザ処理装置１００に提供するソフトウェア提供手段とを有する情報提供機関を含み、課金センタ２００は、ユーザ処理装置１００から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置１００が使用するソフトウェアに対する課金を行う課金手段２４０と、課金処理が終了した時点で、第１の暗号化手段で用いられた第１の復号・秘密鍵をユーザ処理装置１００に送信する復号鍵送信手段２５０とを有し、ユーザ処理装置１００は、予め、課金センタ２００に対して自装置ＩＤを登録するＩＤ登録手段１０１と、配付されたソフトウェアを使用するソフトウェア使用通知を課金センタ２００に通知する使用通知手段１２０と、課金センタ２００から受信した第１の復号秘密鍵を用いてソフトウェアの全部または、一部暗号化された領域を復号し、実行する第１の復号手段１３０とを有する。

【００１８】また、本発明において、課金センタ２００の課金手段２４０は、課金対象となるソフトウェア毎に、ソフトウェアＩＤ、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を格納するための課金情報記憶手段と、ユーザ毎に、被課金者ＩＤ及び、ユーザ課金情報を保持するユーザ情報記憶手段と、ソフトウェアＩＤを用いて、課金情報記憶手段を検索して、ソフトウェア使用料、及び第１の復号・秘密鍵を取得する第１の検索手段と、ユーザ処理装置１００から使用通知手段１２０により送信された被課金者ＩＤに基づいてユーザ情報記憶手段を検索し、該被課金者ＩＤに対応するユーザ課金情報を取得して、ソフトウェア使用料で更新する第１の課金情報更新手段とを含む。

【００１９】また、本発明のユーザ処理装置１００の通知手段は、乱数を生成する乱数生成手段と、課金センタ２００に、ソフトウェア使用通知と共に、乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、第１の復号手段１３０は、課金センタ２００から受信する乱数と乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、課金センタ２００の復号鍵送信手段２５０は、乱数送信手段によりユーザ処理装置１００から受信した乱数を第１の復号・秘密鍵と共に送信する乱数送信手段を含む。

【００２０】また、本発明の課金センタ２００の課金情報記憶手段は、ソフトウェアに対応する第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、復号鍵送信手段２５０は、第２の秘密鍵を用いて、ユーザ処理装置１００に送信する第１の復号・秘密鍵を暗号化した暗号化情報を生成する第２の暗号化手段を含み、ユーザ処理装置１００の第１の復号手段１３０は、課金センタ２００から受信した暗号化情報を、ソフトウェアに埋め込んである第２の秘密鍵を抽出し、暗号化情報を復号して第１の復号・秘密鍵を取得し、該第１の復号・秘密鍵でソフトウェアを復号する第２の復号化手段を含む。

【００２１】また、本発明のユーザ処理装置１００の使用通知手段１２０は、被課金者の第３の私的秘密鍵を用いて、課金センタ２００に送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、課金センタ２００に送信するソフトウェア使用通知と共に署名を課金センタ２００に送信する署名送信手段を更に有し、課金センタ２００は、ユーザ情報記憶手段に、被課金者の第３の私的秘密鍵に対応した公開鍵を含み、ユーザ情報記憶手段上の被課金者の第３の私的秘密鍵に対応し、署名を復号するための公開鍵を用いて、ユーザ処理装置１００から受信した署名を復号し、該ユーザ処理装置１００から受信したソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する。

【００２２】また、本発明の第１の復号化手段は、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む。また、本発明の第１の復号化手段は、予め復号したデータを格納する復号データ格納手段と、ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、復号データ格納手段へのアクセスで代替する代替アクセス手段を含む。

【００２３】また、本発明の課金センタ２００は、課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応し、ユーザ処理装置１００に送信され、該課金対象ソフトウェアを復号するための第４の復号・秘密鍵を格納する第２の課金情報記憶手段と、ソフトウェアＩＤ及び機能ＩＤを用いて、第２の課金情報記憶手段を検索して、機能使用料及び第４の復号・秘密鍵を取得する第２の検索手段と、被課金者ＩＤ及び機能使用料を用いて、ユーザ情報記憶手段を検索して、被課金者ＩＤに対応したユーザ課金情報を更新する第２の課金情報更新手段を更に有し、ユーザ処理装置１００は、被課金者ＩＤ及びソフトウェアＩＤと共に、機能ＩＤを課金センタ２００に送信するＩＤ通知手段を更に有する。

【００２４】また、本発明の情報提供機関の第１の暗号

化手段は、ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む。また、本発明の情報提供機関の第１の暗号化手段は、ソフトウェアの機能単位で暗号化する手段を含む。

【００２５】また、本発明の情報提供機関の第１の暗号化手段は、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する手段を含む。また、本発明の情報提供機関の第１の暗号化手段は、ユーザ処理装置１００に提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する手段を含む。

【００２６】上記の各発明では、予め、ユーザに提供するソフトウェアの全部または、一部が、当該ソフトウェアの開発時または、提供の前に暗号化されているものとする。このソフトウェアの一部を暗号化する場合には、あるアドレスの範囲内のデータを暗号化してもよいし、命令部、または、データ部を暗号化してもよいし、あるいは、機能の単位で暗号化してもよい。また、暗号化対象領域の全てを一種類の秘密鍵で暗号化してもよいし、暗号化対象領域を複数の副領域に分け、それぞれの副領域を異なる秘密鍵で暗号化してもよい。このように、種々の方法により暗号化が可能である。

【００２７】また、本発明では、ソフトウェアの提供前に、課金センタの課金情報記憶手段に、ソフトウェアＩＤと、ソフトウェア使用料、及び上記の暗号化されたソフトウェアを復号するための秘密鍵を登録しておく。さらに、ユーザは、ソフトウェアの使用に先立ち、課金センタのユーザ情報テーブルに被課金者ＩＤを登録しておく。

【００２８】ユーザがユーザ処理装置上でソフトウェアを起動し、ソフトウェアの実行前または、実行中に、当該ユーザ処理装置から、ソフトウェアＩＤ及び被課金者ＩＤを課金センタに送信すると、課金センタでは課金情報記憶手段を、ユーザ処理装置から受信したソフトウェアＩＤを用いて検索し、ソフトウェアの使用料及び復号するための秘密鍵を取得する。次に、課金センタのユーザ課金情報を、ユーザ処理装置から受信した被課金者ＩＤを用いてユーザ情報記憶手段を検索し、課金情報テーブルから取得したソフトウェア使用料を用いて被課金者のユーザ課金情報を更新することにより、被課金者毎の課金処理を行う。さらに、課金センタは、ユーザ処理装置に課金情報記憶手段から取得した復号するための秘密鍵を送信する。これにより、ユーザ処理装置は、課金センタから受信した秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００２９】これにより、情報提供機関から暗号化されたソフトウェアを提供し、ユーザが当該ソフトウェアを実行する（起動する）際に、課金センタにおいて課金処理を行い、当該ソフトウェアを使用するための秘密鍵を送信することにより、ユーザに当該ソフトウェアの使用を許可する。

【００３０】さらに、ソフトウェアの一部を暗号化して送信することにより、ユーザが全てのソフトウェアを利用しない場合に、ユーザは、使用しないソフトウェアに対する支払いを行う必要がない。また、本発明は、ユーザ処理装置において生成した乱数を課金センタに送信し、課金センタから返却された乱数とを照合して、一致する場合のみソフトウェアの復号を行うことにより、第三者の不正使用を防止する。

【００３１】また、本発明は、ソフトウェアを復号するための第１の復号秘密鍵を更に暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、当該暗号化情報を復号して取得した第１の復号鍵を用いて、ソフトウェアを復号して実行することにより、ユーザは、課金センタから受信した暗号化情報を復号できない限りソフトウェアを復号することができない。

【００３２】また、本発明は、ユーザ処理装置において署名を生成して課金センタに送信し、課金センタにおいて、署名を復号した情報と受信した他の情報が一致しているかを判定し、不一致の場合にはユーザ処理装置に第１の復号秘密鍵を送信しないため、悪意の第三者が別の署名を送信した場合には、ソフトウェアを復号し、実行することができない。

【００３３】また、本発明は、復号されたデータを格納する領域を設定しておくことにより、復号されたソフトウェアを順次当該領域に格納しておくことにより、実行時におけるソフトウェアのアクセスを当該領域に対して行うことにより、既に復号されているソフトウェアが格納されているため効率のよいアクセスが可能となる。

【００３４】また、本発明は、ユーザ処理装置から課金センタにソフトウェアＩＤや被課金者ＩＤと共に、ソフトウェアの機能ＩＤを併せて送信することにより、起動するソフトウェア内の機能群単位に課金することが可能となる。

【００３５】

【発明の実施の形態】図３は、本発明のシステム構成図である。以下に説明するシステムは、ユーザ処理装置１００と課金センタ２００及び当該ユーザ処理装置１００と課金センタ２００を接続する通信網（図示せず）から構成される。

【００３６】なお、課金センタ２００は、当該ソフトウェアを提供する情報提供業者であり、課金システムを実行することから便宜的に課金センタと記すものとするが、情報提供業者と課金センタは別個に独立して設定されていもよい。ユーザ処理装置１００は、課金センタ送信部１２０と復号部１３０とを有し、復号部１３０は、課金対象となるソフトウェア１１０を復号鍵（以下、第１の復号・秘密該）を用いて復号する。ソフトウェア１

１０は、その全部または、一部が１つまたは、複数の秘密鍵を用いて暗号化されているものであり、予め課金センタ２００（情報提供業者）から提供されているものとする。

【００３７】課金センタ送信部１２０は、自装置の被課金者ＩＤ等のユーザ情報及び起動するソフトウェアＩＤを送信する。課金センタ２００は、課金情報テーブル２１０、ユーザ情報テーブル２２０、課金情報テーブル検索部２３０、ユーザ課金情報更新部２４０、ユーザ処理装置送信部２５０とを有する。

【００３８】課金情報テーブル２１０は、ソフトウェアＩＤ，ソフトウェア使用料、暗号化されたソフトウェアを復号するための第１の復号秘密鍵から構成される。なお、以下の説明では、情報提供業者から、予め、ユーザ処理装置１００に配付するためのソフトウェアの全部または、一部を暗号化してユーザ処理装置１００に送信し、暗号化時に使用した秘密鍵を第１の復号秘密鍵として、課金センタ２００の課金情報テーブル２１０に登録しておくものとする。

【００３９】ユーザ情報テーブル２２０は、ユーザ処理装置１００から転送された被課金者ＩＤと、ユーザ課金情報とから構成される。課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料を取得し、ユーザ課金情報更新部２４０に転送し、さらに、検索により、第１の復号秘密鍵を取得して、ユーザ処理装置送信部２５０に転送する。

【００４０】ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、ソフトウェアの使用料で更新する。ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に転送する。

【００４１】

【実施例】以下、図面と共に、本発明の実施例を詳細に説明する。

［第１の実施例］本実施例におけるシステム構成は、前述の図３に示すシステム構成によるものである。

【００４２】図４は、本発明の第１の実施例の動作を説明するための図である。

ステップ１０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ１０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００４３】ステップ１０３）　ユーザ処理装置１００において、予め暗号化されたソフトウェア１１０を起動すると、ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤとを課金センタ２００に送信する。

ステップ１０４）　課金センタ２００は、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤとを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

【００４４】ステップ１０５）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤを用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００４５】ステップ１０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０で検索された第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ１０７）　ユーザ処理装置１００は、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００４６】このように、本実施例によれば、ユーザ処理装置１００からソフトウェア使用通知としてソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送出することにより、課金センタからソフトウェアを復号するための第１の復号・秘密鍵を受け取り、暗号化されているソフトウェアを復号して実行することができる。

【００４７】［第２の実施例］本実施例は、乱数を用いてソフトウェアの復号を許可することが可能か否かを判定する処理を前述の第１の実施例に付加したものである。図５は、本発明の第２の実施例のシステム構成図である。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。

【００４８】同図に示す構成は、前述の図３のシステム構成において、ユーザ処理装置１００に乱数を生成する乱数生成部１４０と比較部１５０とを具備し、課金センタ２００に乱数受信部２６０を具備する構成である。ユーザ処理装置１００の乱数生成部１４０は、乱数を生成し、当該乱数を課金センタ送信部１２０に転送し、課金センタ送信部１２０から課金センタ２００に送信する。比較部１５０は、課金センタ２００から戻された乱数と、乱数生成部１４０で生成された乱数と課金センタ２００から返却された乱数とを比較し、一致している場合に、復号部１２０に対してソフトウェア１００の復号を許可する。

【００４９】課金センタ２００の乱数受信部２６０は、ユーザ処理装置１００から取得した乱数をユーザ処理装置送信部２５０を介してユーザ処理装置１００に戻す処理を行う。

【００５０】図６は、本発明の第２の実施例の動作を説

明するための図である。

ステップ２０１）　ユーザ処理装置１００は、予め情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ２０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００５１】ステップ２０３）　乱数生成部１４０は、乱数を生成し、課金センタ送信部１２０に転送する。

ステップ２０４）　課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤ及び、乱数とを課金センタ２００に送信する。

【００５２】ステップ２０５）　課金センタ２００において、乱数受信部２６０は、乱数を受信し、第１の実施例と同様に、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

【００５３】ステップ２０６）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤ用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００５４】ステップ２０７）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０で検索された第１の復号秘密鍵と乱数受信部２６０で受信した乱数をユーザ処理装置１００に送信する。

ステップ２０８）　ユーザ処理装置１００は、課金センタ２００から受信した乱数とステップ２０３で生成された乱数とを比較し、一致する場合には、復号部１３０において、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００５５】本実施例では、ユーザ処理層１００から課金センタ２００に送信した乱数と、課金センタ２００から受信した乱数とが一致したときのみソフトウェアの復号を可能とする。

［第３の実施例］本実施例のシステム構成は、基本的に図３に示す構成と同様であるが、課金情報テーブル２１０において、第２の秘密鍵を保持し、課金情報テーブル検索部２３０においてソフトウェアＩＤに基づいて当該第２の秘密鍵を検索し、ユーザ課金情報更新部２４０において、第１の復号・秘密鍵を暗号化する点において異なる。

【００５６】図７は、本発明の第３の実施例の動作を説明するための図である。

ステップ３０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ３０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００５７】ステップ３０３）　課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送信する。

ステップ３０４）　課金センタ２００は、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料、第１の復号秘密鍵及び、第２の秘密鍵とを取得する。

【００５８】ステップ３０５）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤを用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００５９】ステップ３０６）　さらに、ユーザ課金情報更新部２４０は、第１の復号秘密鍵を課金情報テーブル２１０から取得した第２の秘密鍵を用いて暗号化し、ユーザ処理装置送信部２５０に転送する。

ステップ３０７）　ユーザ処理装置送信部２５０は、ユーザ課金情報更新部２４０で暗号化された情報をユーザ処理装置１００に送信する。

【００６０】ステップ３０８）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した暗号化された情報、ソフトウェア１１０に埋め込まれている第２の秘密鍵を用いて復号し、第１の復号秘密鍵を取得する。

ステップ３０９）　さらに、復号部１３０は、ステップ３０８で復号することにより取得した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００６１】このように、本実施例によれば、第１の復号・秘密鍵を暗号化してユーザ処理装置に送信することにより、より安全な第１の復号・秘密鍵を送信することができる。

［第４の実施例］図８は、本発明の第４の実施例のシステム構成図である。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。

【００６２】図８に示すシステムにおいて、図３と異なる構成は、ユーザ処理装置１００においては、第３の私的秘密鍵保持部１６０と署名生成部１７０を含む点である。第３の私的秘密鍵保持部１６０は、署名を生成するための第３の私的秘密鍵を保持する。署名生成部１７０は、第３の私的秘密鍵を用いて署名を生成する。

【００６３】また、課金センタ２００のユーザ情報テーブル２２０は、被課金者ＩＤ、課金情報に加えて、署名

を復号するための公開鍵を保持する。図９は、本発明の第４の実施例のユーザ課金情報更新部の詳細な構成を示す。同図に示すユーザ課金情報更新部２４０は、ユーザ情報テーブルを検索し、公開鍵を取得するテーブル検索部２４１、ユーザ処理装置１００から取得した署名を公開鍵を用いて復号する署名復号部２４２、ユーザ処理装置１００から受信した他の情報と復号された情報とが一致しているかを比較する比較部２４３、ユーザ情報テーブル２２０を更新するテーブル更新部２４４から構成される。

【００６４】テーブル更新部２４４は、比較部２４３において、復号化情報と、ユーザ処理装置１００から受信した情報が一致している場合に限り、被課金者のユーザ課金情報を課金情報テーブル検索部２３０から取得したソフトウェア使用料で更新し、さらに、テーブル検索部２４１から取得した、第１の復号秘密鍵をユーザ処理装置送信部２５０に転送する。

【００６５】図１０は、本発明の第４の実施例の動作を説明するための図である。

ステップ４０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ４０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００６６】ステップ４０３）　ユーザ処理装置１００の署名生成部１７０は、第３の私的秘密鍵保持部１６０から第３の私的秘密鍵を読み出して、ソフトウェアＩＤ，被課金者ＩＤとの一部を当該第３の私的秘密鍵を用いて暗号化することにより、署名を生成し、課金センタ送信部１２０に転送する。

【００６７】ステップ４０４）　課金センタ送信部１２０は、暗号化されたソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送信する。

ステップ４０５）　ユーザ課金情報更新部２４０のテーブル検索部２４１は、受信した暗号化情報に対して、ユーザ情報テーブル２２０を検索して公開鍵を取得して署名復号部２４２に転送する。署名復号部２４２は、当該被課金者の公開鍵を取得し、当該暗号化情報を公開鍵で復号し、比較部２４３に転送する。比較部２４３は、ユーザ処理装置１００から受信した他の情報と比較し、一致しているかを判定する。一致している場合には、次のステップに移行する。

【００６８】ステップ４０６）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤと被課金者ＩＤを用いて、課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料、第１の復号秘密鍵とを取得する。

【００６９】ステップ４０７）　ユーザ課金情報更新部２４０のテーブル更新部２４４は、課金情報テーブル検索部２３０からユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００７０】ステップ４０８）　さらに、ユーザ課金情報更新部２４０は、第１の復号秘密鍵をユーザ処理装置送信部２５０に転送し、ユーザ処理装置送信部２５０は、ユーザ課金情報更新部２４０で暗号化された情報をユーザ処理装置１００に送信する。

【００７１】ステップ４０９）　ユーザ処理装置１００の復号部１３０は、第１の復号秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。なお、本発明は、前述の各実施例と組み合わせて実行することも可能である。これにより、署名と一致しない場合には、課金センタ２００からユーザ処理装置１００に第１の復号・秘密鍵を送信しないため、正当な署名を持たない限り、ユーザは、ソフトウェアを復号できない。

【００７２】［第５の実施例］本実施例におけるシステム構成は、図３と基本的に同様である。図１１は、本発明の第５の実施例の動作を説明するための図である。

ステップ５０１）　ユーザ処理装置１００において、予め命令部分が暗号化されたソフトウェア１１０を起動する。

【００７３】ステップ５０２）　ユーザ処理装置１００は、ソフトウェア１００をロードする。

ステップ５０３）　ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤ，被課金者ＩＤとを課金センタ２００に送信する。

【００７４】ステップ５０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

ステップ５０５）　ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、被課金者のユーザ課金情報を課金情報テーブル２１０から取得したソフトウェア使用料で更新する。

【００７５】ステップ５０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ５０７）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した第１の復号秘密鍵を用いて、次に実行する命令を読み出す。

【００７６】ステップ５０８）　復号部１３０は、読み出した命令を復号する。

ステップ５０９）　復号部１３０により復号された命令を実行する。

ステップ５０８とステップ５０９の処理を当該復号され

た命令の全てが終了するまで繰り返す。

【００７７】［第６の実施例］図１２は、本発明の第６の実施例のユーザ処理装置の構成を示す。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。なお、本実施例は、図３の構成と同様である。

【００７８】図１２において、ユーザ処理装置１００は、図３の構成に、復号部１３０で復号された命令を格納する復号済ソフトウェア格納部１８０と、当該復号済ソフトウェア格納部１８０に格納されている命令を順次読み出して実行する実行部１９０が付加されたものである。

【００７９】図１３は、本発明の第６の実施例の動作を説明するための図である。

ステップ６０１）　ユーザ処理装置１００において、予め命令部分が暗号化されたソフトウェア１１０を起動する。

ステップ６０２）　ユーザ処理装置１００は、ソフトウェア１００をロードする。

【００８０】ステップ６０３）　ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤ，被課金者ＩＤとを課金センタ２００に送信する。

ステップ６０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

【００８１】ステップ６０５）　ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、被課金者のユーザ課金情報を課金情報テーブル２１０から取得したソフトウェア使用料で更新する。

【００８２】ステップ６０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ６０７）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号する。

【００８３】ステップ６０８）　復号部１３０は、復号したソフトウェアを復号済ソフトウェア格納部１８０に格納する。

ステップ６０９）　実行部１９０は、復号済ソフトウェア格納部１８０にアクセスし、復号されたソフトウェアを実行する。

【００８４】［第７の実施例］本実施例における課金情報テーブル２１０は、ソフトウェアＩＤ、機能に対応した機能ＩＤ，機能に対応した使用量と、機能に対応し、暗号化されているソフトウェアの全部又は一部の領域として復号するための第４の復号・秘密鍵とを含むもの構成である。第４の復号・秘密鍵は、ユーザ処理装置１００に送信され、ソフトウェア１１０を復号するための鍵である。

【００８５】図１４は、本発明の第７の実施例の動作を説明するための図である。

ステップ７０１）　ユーザ処理装置１００は、予め機能毎に異なる秘密鍵を用いて暗号化されたソフトウェアを起動する。

ステップ７０２）　起動したソフトウェアをメモリ上にロードする。

【００８６】ステップ７０３）　ユーザ処理装置１００の課金センタ送信部１２０は、実行しようとする機能の機能ＩＤ（機能Ａ）と、ソフトウェアＩＤと、被課金者ＩＤとを課金センタ２００に送信する。

ステップ７０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置から受信したソフトウェアＩＤと、機能ＩＤとを用いて、課金情報テーブル２１０を検索し、当該機能の使用料と、第４の復号秘密鍵を取得する。

【００８７】ステップ７０５）　ユーザ課金情報更新部２４０は、課金情報テーブル検索部２３０により取得された機能使用料でユーザ情報テーブル２２０を更新する。

ステップ７０６）　ユーザ処理装置送信部２５０は、課金情報テーブル２１０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

【００８８】ステップ７０７）　ユーザ処理装置１００は、課金センタ２００から受信した第１の復号秘密鍵を用いて、当該機能の全部または、一部の暗号化されているソフトウェアの領域を復号して実行する。上記の手順を、当該ソフトウェアを使用してユーザが必要とする処理が終了するまで、機能の単位で繰り返す。ステップ７０８以降は、ユーザ処理装置１００から機能ＩＤとして“機能Ｂ”を課金センタ２００に送信して、上記のステップ７０４～ステップ７０７と同様の処理を繰り返すものである。

【００８９】なお、上記の各実施例において、ユーザ課金情報としては、前納方式、後納方式、累積課金方式、明細課金方式及びクレジット支払い方式のいずれにも適用可能である。また、上記の各実施例において、ソフトウェアをプログラムとして説明しているが、この例に限定されることなく、プログラムに留まらず、音声情報、映像除法、画像情報、テキスト情報を含む全てのディジタル情報に対して適用可能である。

【００９０】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００９１】

【発明の効果】上述のように、本発明のソフトウェア課金方法及びシステムによれば、どの時点においても暗号

化されている部分を含まないソフトウェアが、メモリ及びディスク等の記憶媒体上に存在しないため、ソフトウェアの反復使用を確実に阻止することができ、ソフトウェアの使用の都度、確実に使用料を徴収することが可能となるため、ユーザは必要な機能のみを安価な使用料で使用することが可能となる。

【００９２】また、ソフトウェアの暗号化に用いる秘密鍵の個数と暗号化の範囲を選択することにより、起動するソフトウェアの単位で課金することも、起動するソフトウェア内の機能群単位に課金することも可能となる。また、使用料前払い、または、使用限度額に基づくクレジットを課金センタに登録して使用料残高を管理することにより、使用料の徴収漏れを防止することが可能となる。

【００９３】また、ユーザ処理装置から課金センタに送信する時に添付した、乱数と課金センタからユーザ処理装置に送信する時に添付された乱数との一致を検証することにより、課金センタからユーザ処理装置に送信された情報を横取りすることによるソフトウェアの不正使用を防止することが可能となる。

【００９４】また、課金センタからユーザ処理装置に送信において、公開暗号方式を利用し、署名を添付することにより、他人の被課金者ＩＤを使用したソフトウェアの不正使用を防止することが可能となる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明のシステム構成図である。

【図４】本発明の第１の実施例の動作を説明するための図である。

【図５】本発明の第２の実施例のシステム構成図である。

【図６】本発明の第２の実施例の動作を説明するための図である。

【図７】本発明の第３の実施例の動作を説明するための図である。

【図８】本発明の第４の実施例のシステム構成図である。

【図９】本発明の第４の実施例のユーザ課金情報更新部の構成図である。

【図１０】本発明の第４の実施例の動作を説明するための図である。

【図１１】本発明の第５の実施例の動作を説明するための図である。

【図１２】本発明の第６の実施例のユーザ処理装置の構成図である。

【図１３】本発明の第６の実施例の動作を説明するための図である。

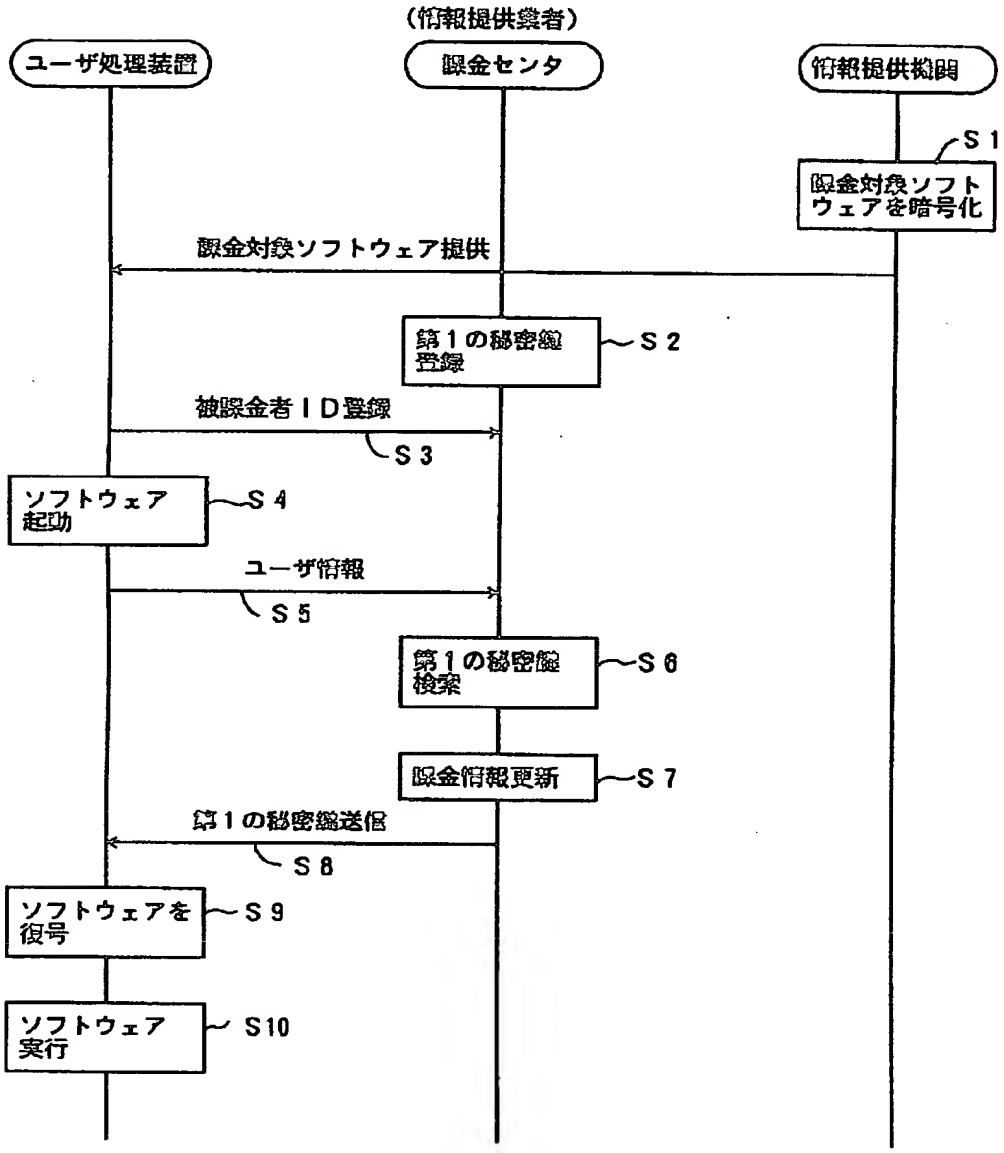
【図１４】本発明の第７の実施例の動作を説明するための図である。

【符号の説明】

１００　ユーザ処理装置
１０１　ＩＤ登録手段
１１０　ソフトウェア
１２０　課金センタ送信部、使用通知手段
１３０　復号部、第１の復号・秘密手段
１４０　乱数生成部
１５０　比較部
１６０　第３の秘密鍵保持部
１７０　署名生成部
１８０　復号済ソフトウェア格納部
１９０　実行部
２００　課金センタ
２０１　第１の暗号化手段
２０２　ソフトウェア提供手段
２１０　課金情報テーブル
２２０　ユーザ情報テーブル
２３０　課金情報テーブル検索部
２４０　ユーザ課金情報更新部、課金手段
２４１　テーブル検索部
２４２　署名復号部
２４３　比較部
２４４　テーブル更新部
２５０　ユーザ処理装置送信部、復号鍵送信手段
２６０　乱数受信部

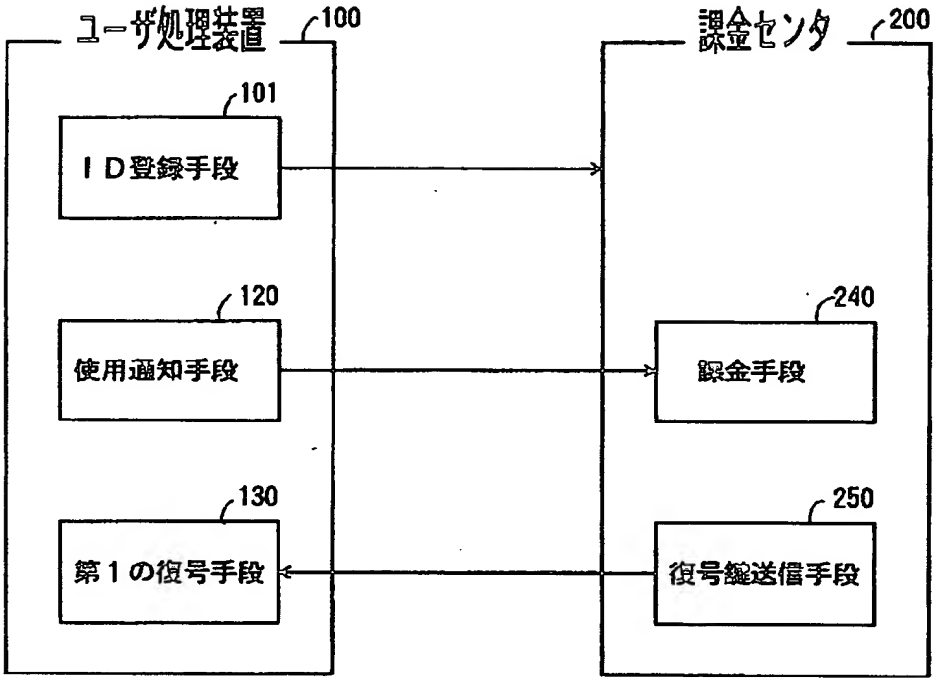
【図１】

本発明の原理を説明するための図



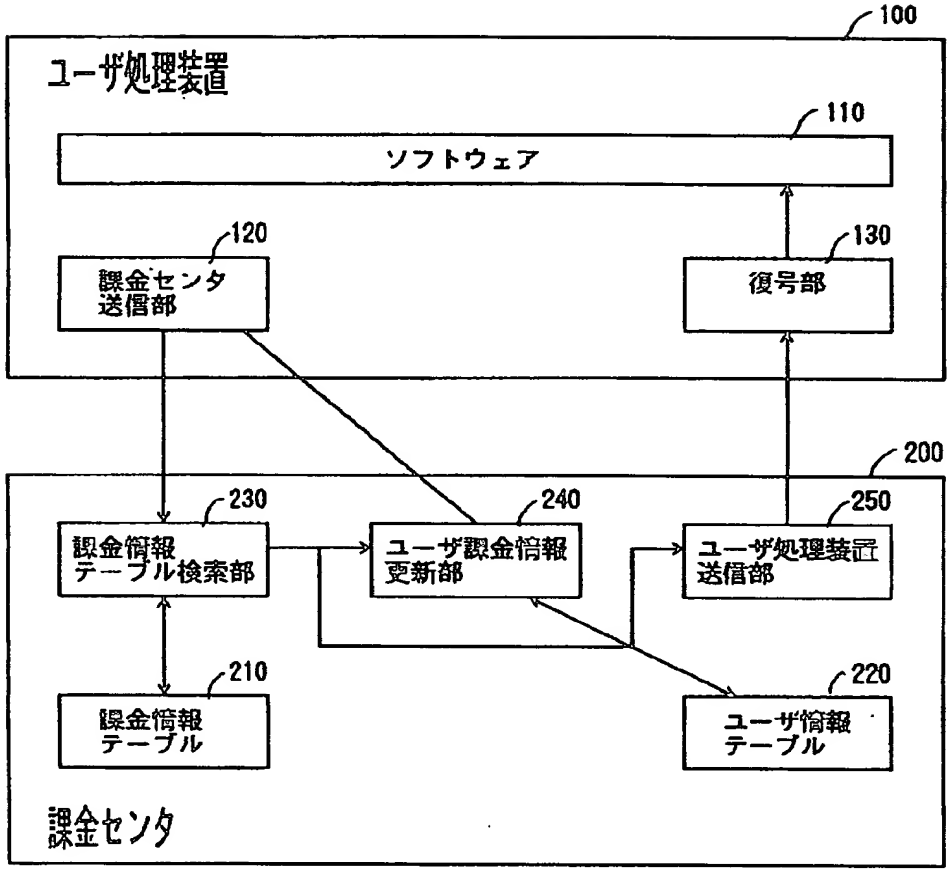
【図２】

本発明の原理構成図



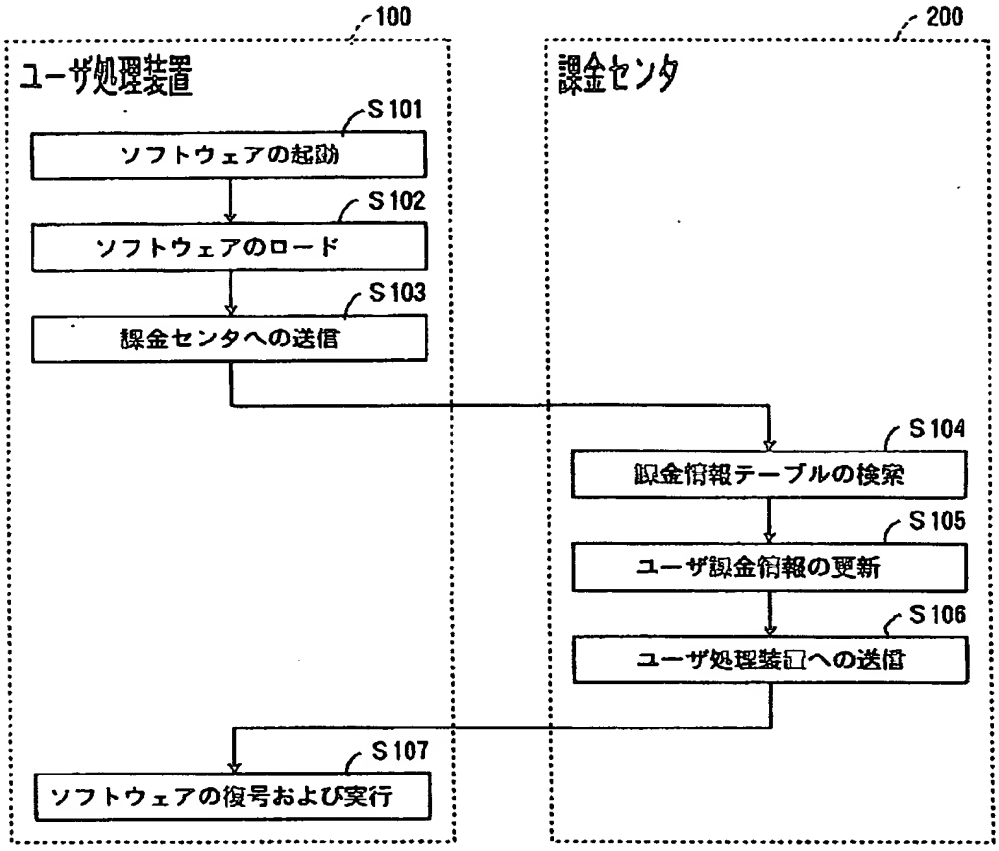
【図３】

本発明のシステム構成図



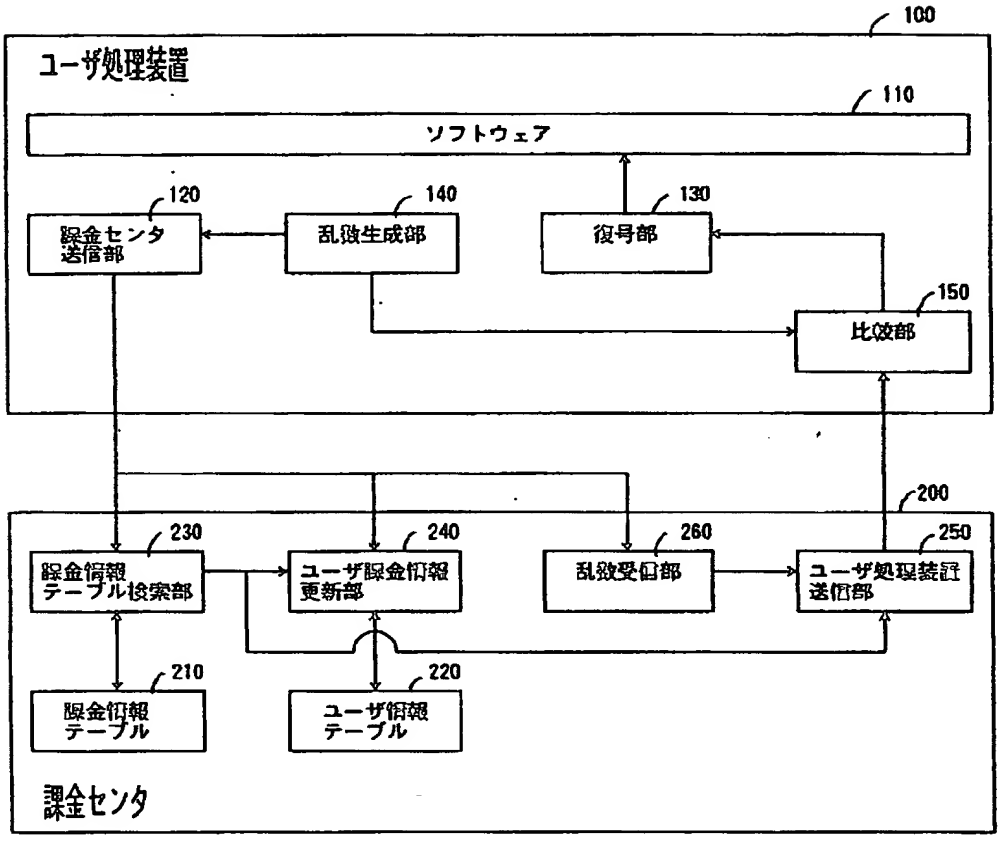
【図４】

本発明の第１の実施例の動作を説明するための図



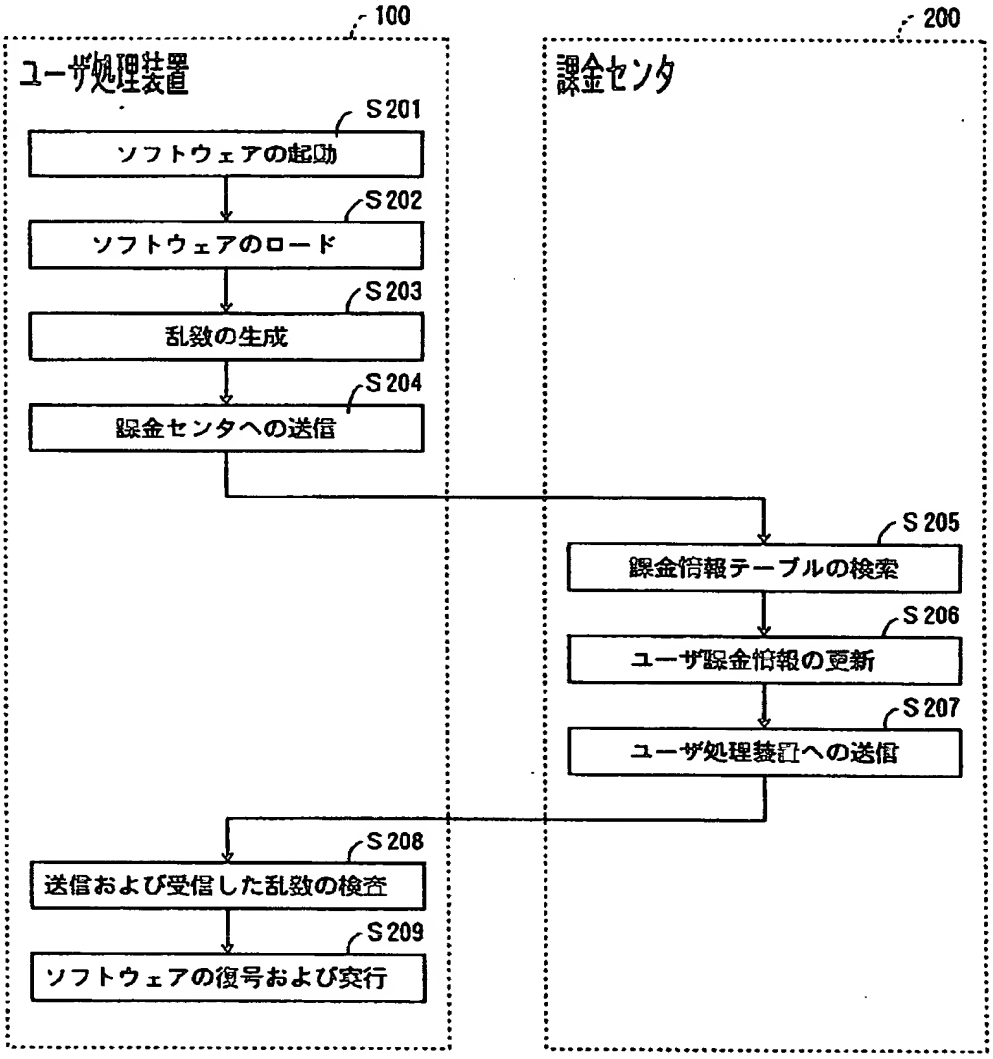
【図５】

本発明の第２の実施例のシステム構成図



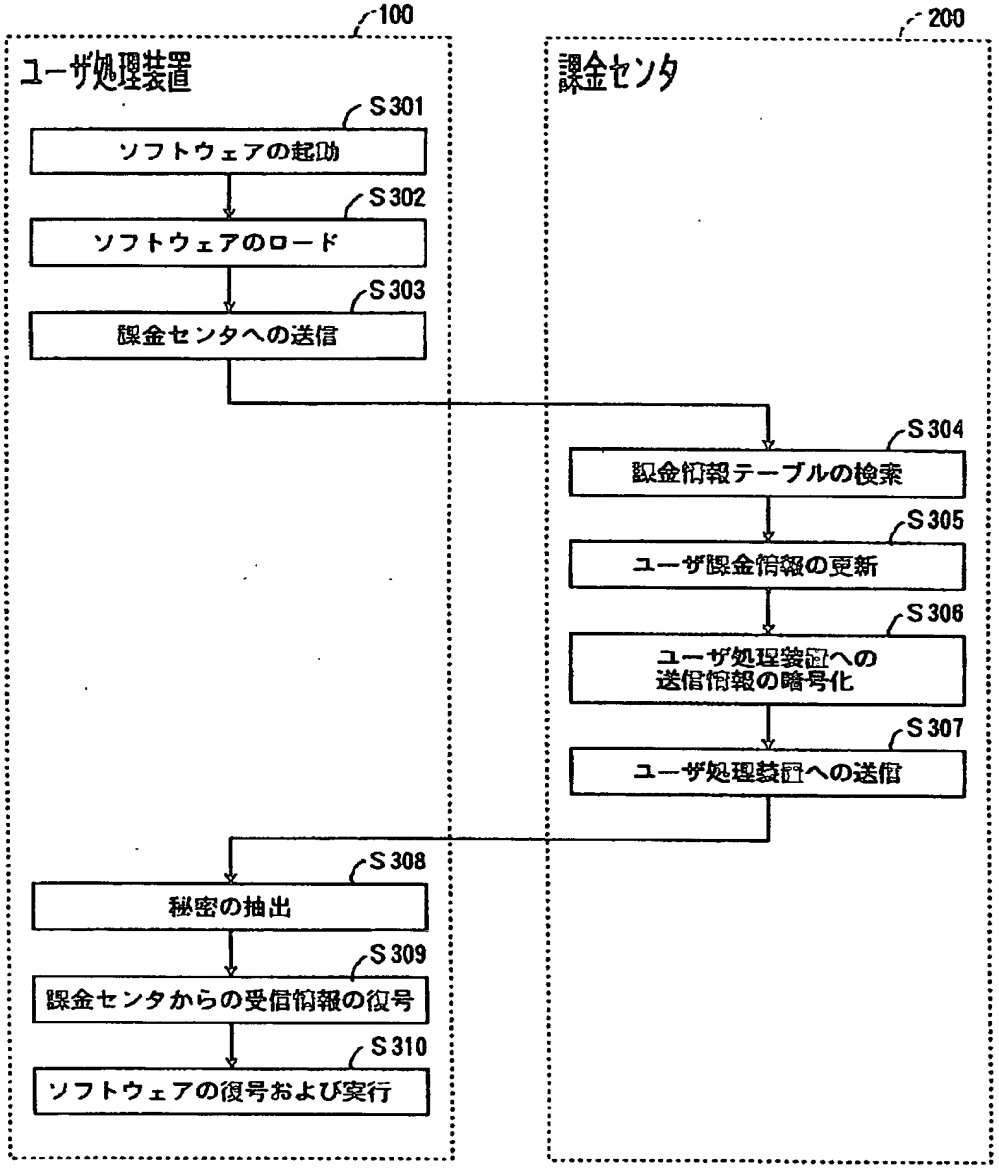
【図６】

本発明の第２の実施例の動作を説明するための図



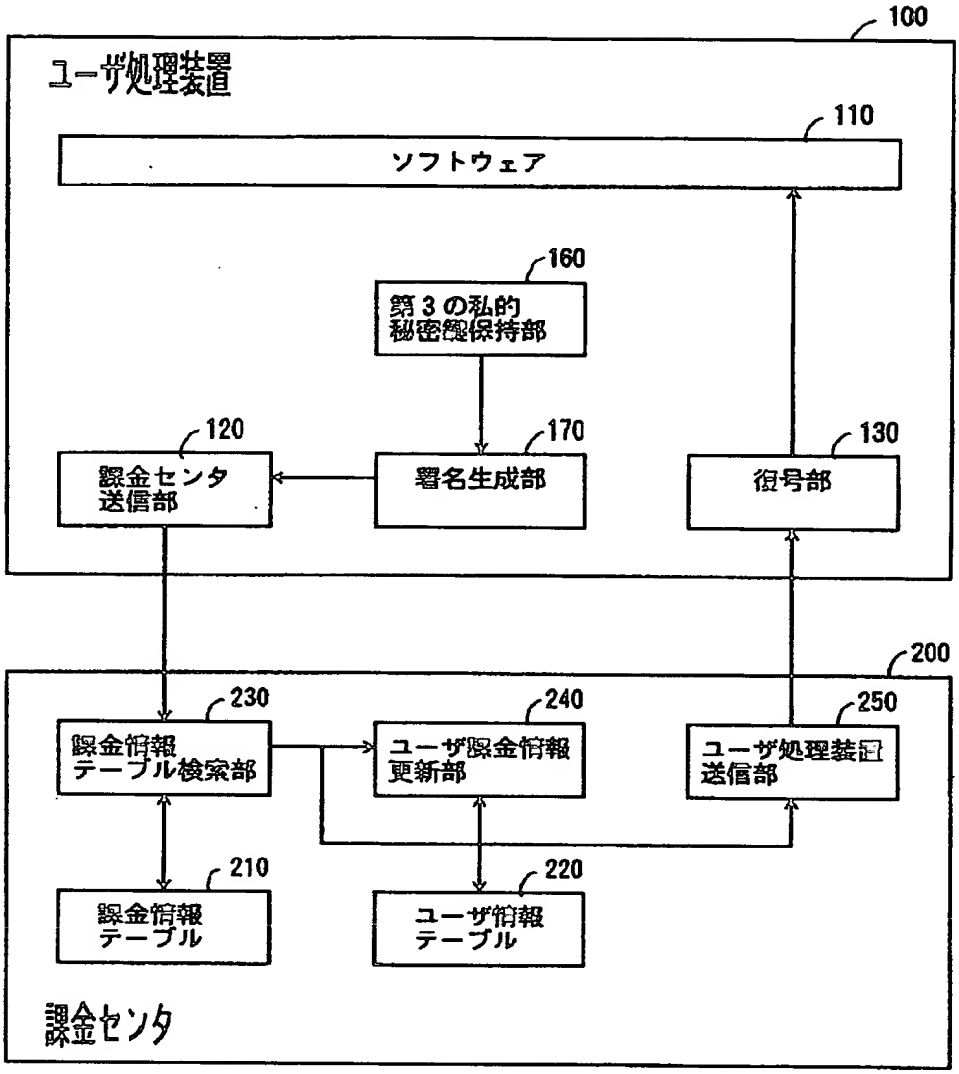
【図７】

本発明の第３の実施例の動作を説明するための図



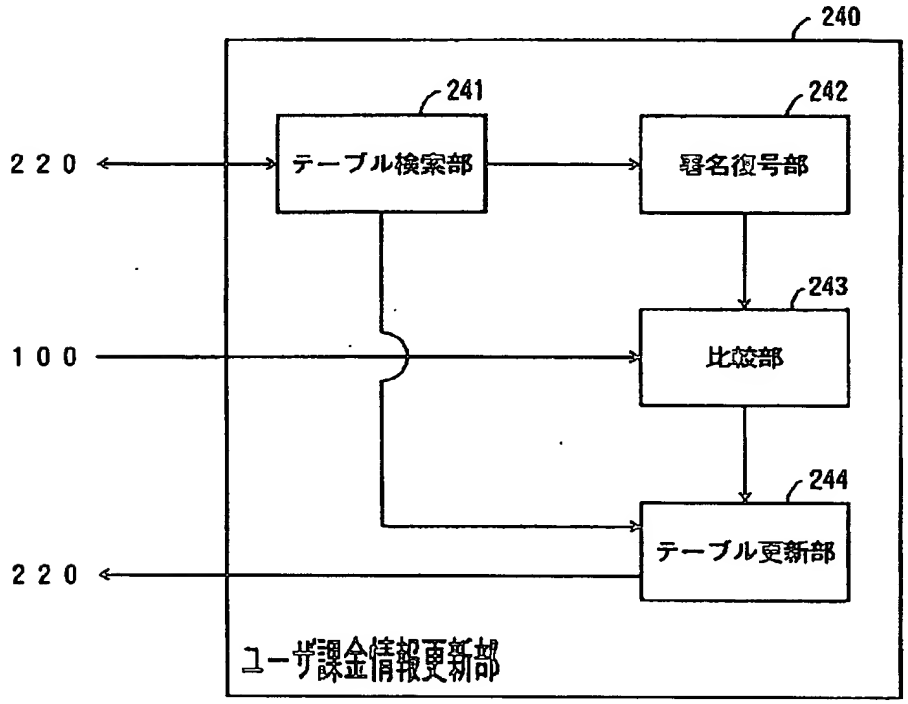
【図８】

本発明の第４の実施例のシステム構成図



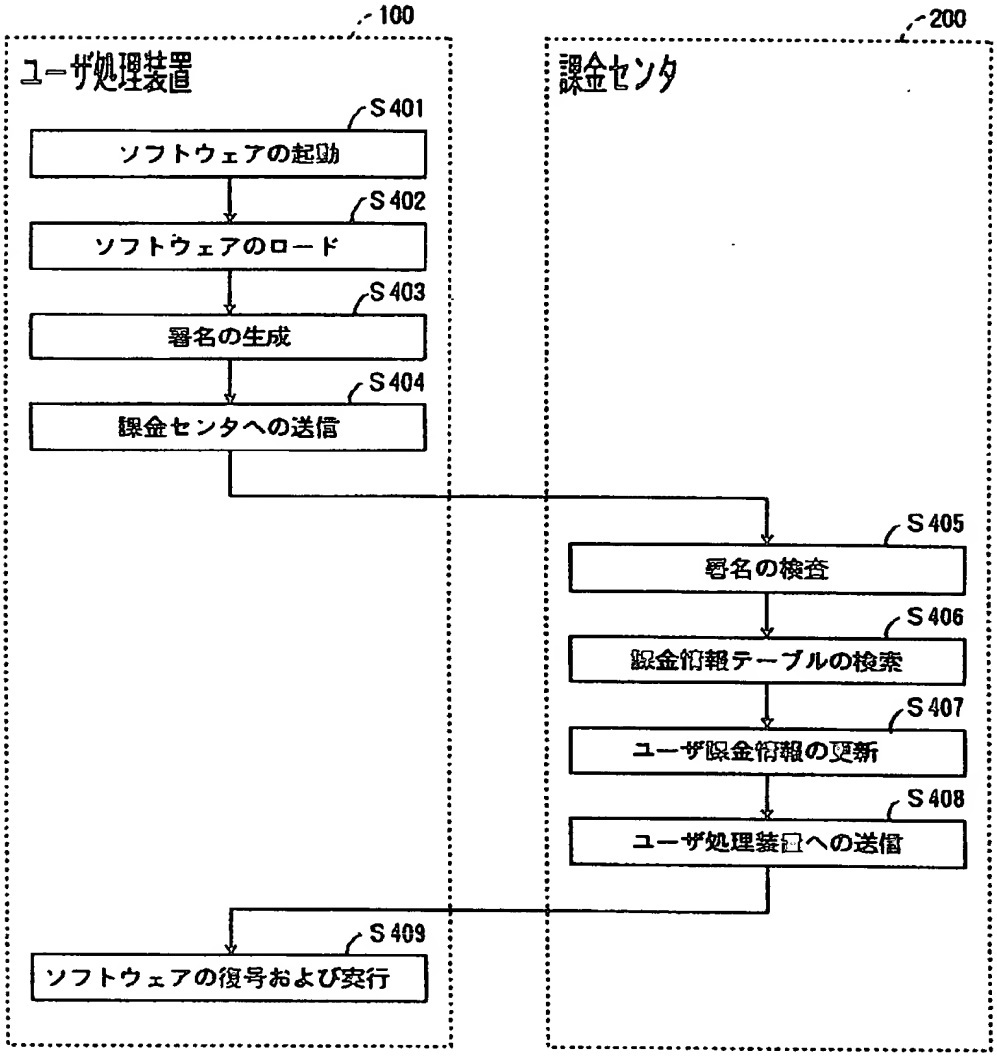
【図９】

本発明の第４の実施例のユーザ課金情報更新部の構成図



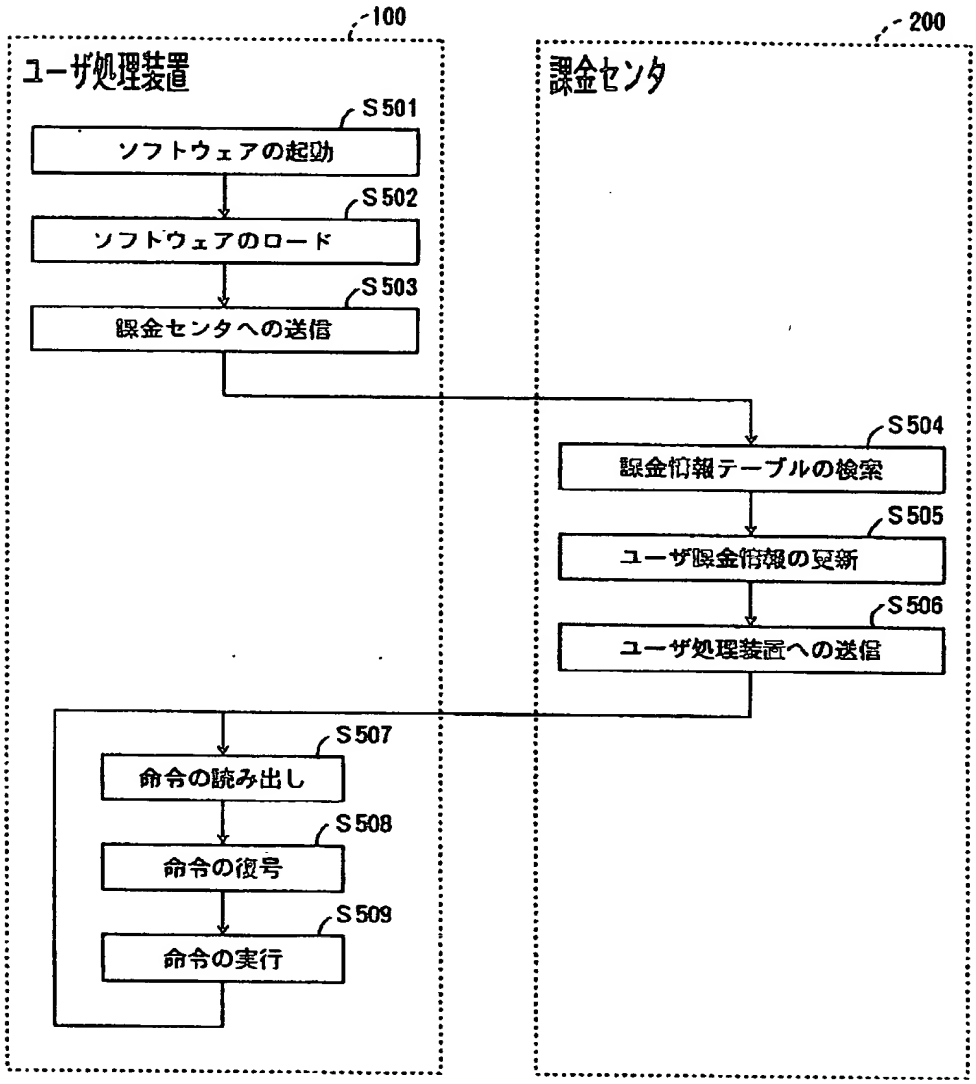
【図１０】

本発明の第４の実施例の動作を説明するための図



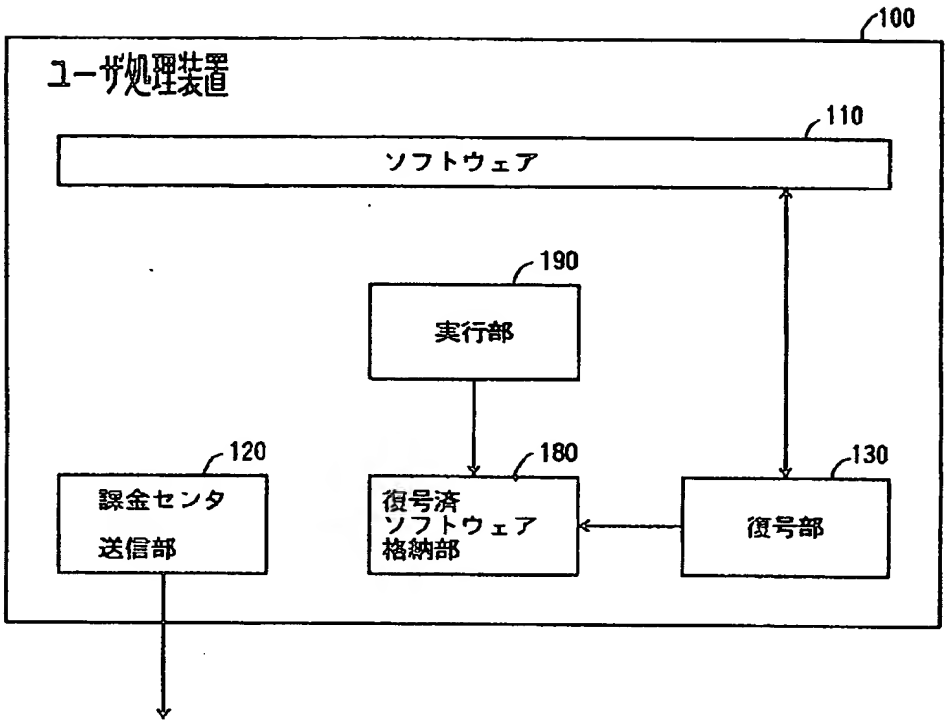
【図１１】

本発明の第５の実施例の動作を説明するための図



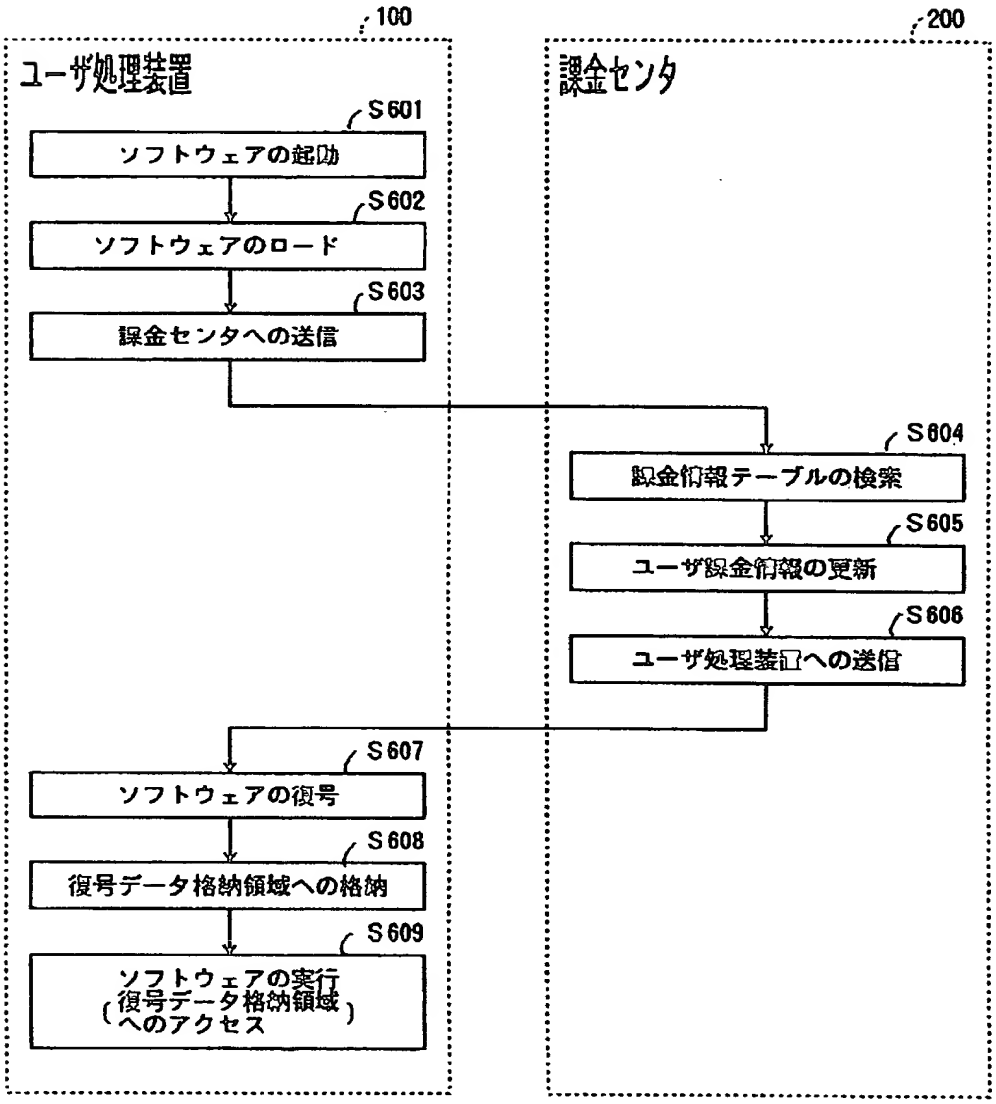
【図１２】

本発明の第６の実施例のユーザ処理装置の構成図



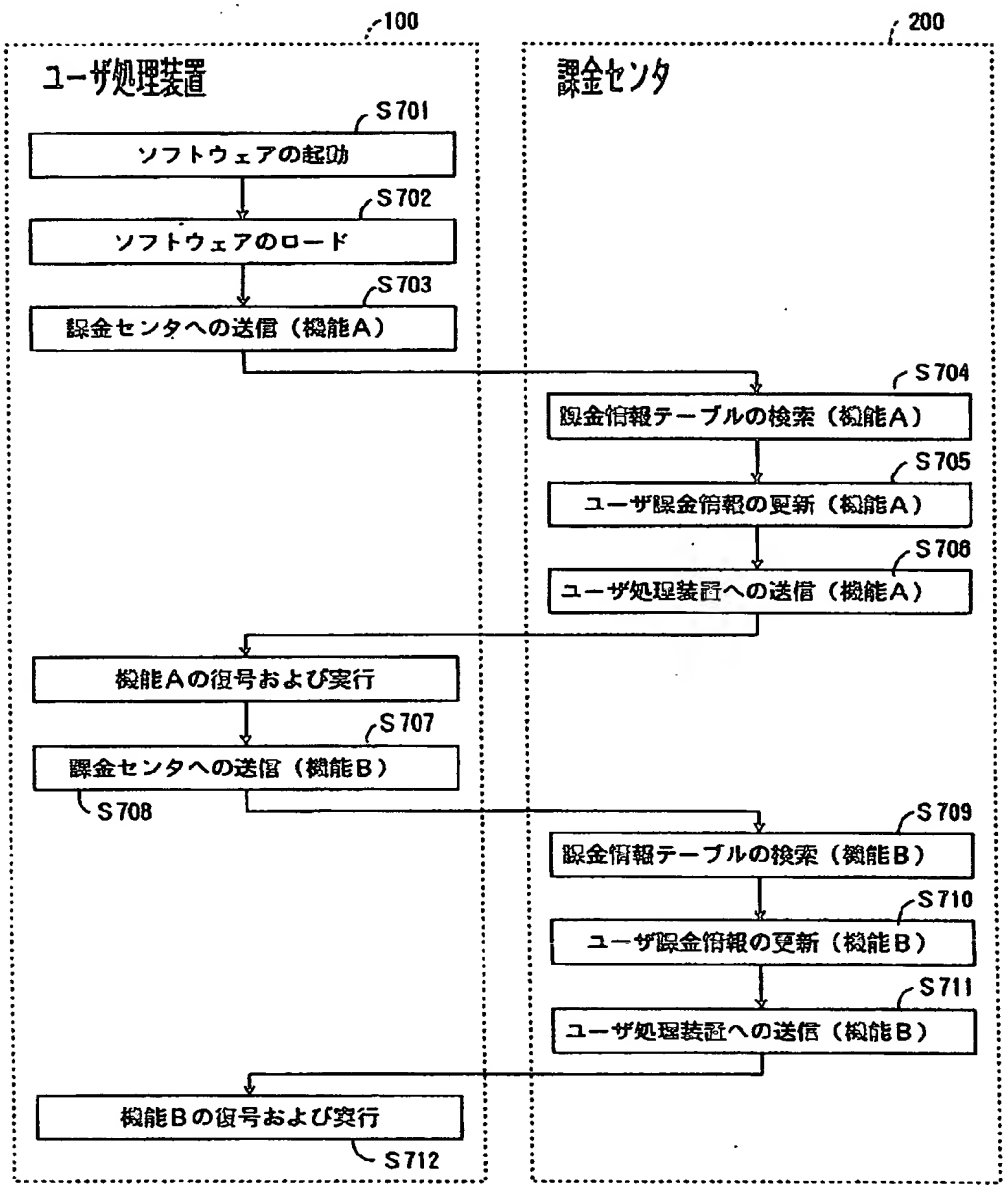
【図１３】

本発明の第６の実施例の動作を説明するための図



【図１４】

本発明の第７の実施例の動作を説明するための図



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	F I		技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ
			7259－5Ｊ			６４０Ｅ
		６６０	7259－5Ｊ			６６０Ｚ
			7259－5Ｊ			６６０Ｄ